Department of Homeland Security Daily Open Source Infrastructure Report for 12 June 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports the Federal Aviation Administration, reacting to a December 2005 accident in which a Southwest Airlines Co. jet skidded off the end of a snowy Chicago runway, have issued new landing policies aimed at preventing such accidents. (See item 8)
- Texas Governor Rick Perry has announced a plan to install hundreds of night−vision cameras on private land along the Mexican border and put the live video on the Internet, so that anyone with a computer who spots illegal immigrants trying to slip across can report it on a toll−free hotline. (See item 11)
- The U.S. Food and Drug Administration has announced new measures that emphasize certain regulatory actions and the use of new technologies for safeguarding the integrity of the U.S. drug supply against the growing problem of counterfeit drugs. (See item 21)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 10, Chicago Tribune* — **Mexican oil industry threatened.** Analysts predict that Mexico's oil reserves, second only to Canada's in filling up U.S. gasoline tanks, could dry up within a dozen years. Meanwhile, Pemex, the state−owned oil company, lacks sufficient money to repair

antiquated pipelines and explore for more deep−sea deposits. One solution would be outside investment. But almost all Mexicans oppose loosening their constitution to allow private or foreign interests to break the government monopoly and hold a stake in the nation's oil. The government takes most Pemex profits to cover a third of the federal budget for schools and other public services. Despite today's high oil prices, Pemex remains the world's most indebted oil company, in hock by as much as $85 billion. While producing 3.4 million barrels of oil a day, it imports gasoline because it lacks refineries.
Source: http://www.mercurynews.com/mld/mercurynews/news/world/147876 85.htm

2. *June 08, KUTV (UT)* — **Power plant owner electrocuted.** The owner of a small power plant in Little Cottonwood Canyon, UT, died as the result of an electrocution, but authorities were still trying to determine how it happened. William Lennon, was found dead at the plant Thursday, June 8, by his wife. An autopsy found he was electrocuted. Lennon went to the plant on Little Cottonwood Creek on Wednesday, June 7, to do maintenance work and never returned.
Source: http://kutv.com/topstories/local_story_159222052.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *June 09, Fine Extra (UK)* — **Disgruntled UBS IT worker accused of unleashing logic bomb on bank network.** A U.S. court has heard how a former IT worker for UBS allegedly unleashed a "logic bomb" computer virus on the bank's network because he was unhappy with his bonus payment. But not only has Roger Duronio, 60, of New Jersey been charged with using the logic bomb to cause more than $3 million in damage to the computer network at UBS's stockbroking unit Paine Webber, he has also been charged with securities fraud for his failed plan to drive down the company's stock with activation of the logic bomb. Duronio resigned from the company on February 22, 2002, and on March 4, 2002, his program activated and began deleting files on over 1000 of UBS PaineWebber's computers. Around 17,000 UBS traders across the U.S. were unable to trade shares for more than a day because of the damage.
Source: http://www.finextra.com/fullstory.asp?id=15420

4. *June 08, VNUNet* — **Nigerian scam moves to Scotland.** A well established e−mail scam that asks people to look after funds for a Nigerian government official has spawned a copycat message from sources closer to home. The e−mail pretends to be from Patricia Ferguson, the

Scottish Minister for Culture, Tourism and Sport, and asks people to help move $40 million for a share of the cash. The e−mail contains links to the Member of the Scottish Parliament's personal Website in an attempt to look genuine, security firm Sophos has warned that it is designed to steal the victim's bank details.
Source: http://www.vnunet.com/vnunet/news/2157790/nigerian−scam−move s−scotland

5. *June 08, Websense Security Labs* — **Phishing Alert: Bank ASYA.** Websense Security Labs has received reports of a new phishing attack that targets customers of Bank ASYA, a Turkish Bank. Users receive a spoofed e−mail, which informs them that upgrades are taking place and that they will have to confirm account details. When users click on the link, they are taken to a phishing site that requests account information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=509

6. *June 08, Websense Security Labs* — **Phishing Alert: Spencer Savings Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of Spencer Savings Bank. Users receive a spoofed e−mail message, which claims that they must confirm their account details. This message provides a link to a phishing Website that prompts users to enter account information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=510

[Return to top]

Transportation and Border Security Sector

7. *June 10, New York Times* — **Mob takes car from U.S. Border Patrol in Ontario.** A mob of American Indian protesters hijacked a United States Border Patrol car in Ontario and then used it to try to run over a Canadian police officer, the Ontario Provincial Police said Saturday, June 10. The hijacking took place Friday, June 9, at the site of a three−month standoff between the Indians, local residents and the police over a land claim in Caledonia, Ontario, said Constable Paula Wright of the Ontario police. Another officer from the Ontario police force told The Canadian Press that the American agents were visiting the scene near the American border, which experienced several violent episodes on Friday, including an attack on a television news crew, to see how Canadian officers were dealing with the situation. According to the Canadian police, a crowd of protesters, angry about a housing development on land that they claim as their own, swarmed the border patrol vehicle and forcibly removed its three occupants. The Ontario police arrested three people immediately after the attack with the car, charging them with breaching the peace. The police force is seeking arrest warrants for seven other people on more serious charges.
Source: http://www.nytimes.com/2006/06/11/world/americas/11ontario.h tml?_r=1&oref=slogin

8. *June 09, Associated Press* — **FAA issues new landing−distance policies after Midway accident.** Federal aviation regulators, reacting to a December 2005 accident in which a Southwest Airlines Co. jet skidded off the end of a snowy Chicago runway, have issued new landing policies aimed at preventing such accidents. Two weeks before a scheduled public hearing about the accident, the Federal Aviation Administration (FAA) has called for more

stringent and uniform pilot calculations to ensure an adequate safety margin when landing jetliners on snowy or slippery runways. The FAA wants at least a 15 percent safety margin when computing landing distances in such adverse weather conditions. The document released earlier this week says an agency investigation prompted by the Boeing Co. 737 accident found that about half of U.S. carriers lacked clear policies "for assessing whether sufficient landing distance" is available when operating on wet or snowy runways. The FAA says it also found that airlines use "inconsistent" safety margins when computing landing distances in such circumstances, including some calculations conflicting with data provided by aircraft manufacturers. By October, according to the FAA policy document, the agency will put out specific operating and training requirements.
Source: http://www.centredaily.com/mld/centredaily/business/14782386 .htm

9. *June 09, Reuters* — **Northwest ground workers ratify labor contract.** A group of ground workers at Northwest have ratified a contract that brings the bankrupt carrier a step closer to the $1.4 billion labor−savings target it says it needs to survive, the workers' union said on Friday, June 9. The deal, which requires approval from the bankruptcy court, will not take effect until Northwest has concessions in place, either ratified or imposed with court approval, with all the unions at the airline. Northwest's flight attendants rejected a contract proposal earlier this week. The airline has deals with its other unionized workers and has asked for court permission to void the flight attendants' current contract and impose new terms.
Source: http://biz.yahoo.com/rb/060609/airlines_northwest.html?.v=3

10. *June 09, Associated Press* — **Delta to recall 60 to 70 furloughed pilots.** Delta Air Lines Inc. said Friday, June 9, it is recalling 60 to 70 furloughed pilots this summer. The Atlanta−based airline, the nation's third−largest carrier, said the move would help Delta meet new schedule demands and add flexibility to ensure good on−time performance. With the move, Delta will have about 6,000 pilots. The airline's pilot ranks have thinned by several thousand over the last five years while Delta lost billions of dollars.
Source: http://biz.yahoo.com/ap/060609/delta_pilots.html?.v=1

11. *June 09, Associated Press* — **Texas to install border Web cameras.** Texas Governor Rick Perry has announced a $5 million plan to install hundreds of night−vision cameras on private land along the Mexican border and put the live video on the Internet, so that anyone with a computer who spots illegal immigrants trying to slip across can report it on a toll−free hotline. Under the plan, cameras and other equipment would be supplied to willing landowners and placed along some of the most remote reaches of the border. The live video would be made available to law enforcement and anyone else with an Internet connection. Viewers would be able to call day or night to report anything that looks like trespassing, drug smuggling or something else suspicious. Border Patrol Chief David Aguilar did not comment directly on the governor's plan Wednesday, June 7, but said: "We are looking forward to the opportunity to sit down and discuss it with him to ensure that whatever is done will be aligned with the efforts of the Border Patrol." Connie Hair, a spokesperson for the Minuteman organization, which patrols the border against illegal immigrants, said access to the video should be restricted to trained volunteers and law enforcement officials, to prevent smugglers from using the equipment to adjust their routes.
Source: http://www.usatoday.com/news/nation/2006−06−09−texas−border− cams_x.htm

12. *June 09, Associated Press* — **Three teens with guns arrested on Washington Metro.** Three teenagers have been arrested by Washington, DC, Metro police for carrying handguns into the transit system. Metro says that just before noon on Friday, June 9, a passenger at the Green Line's Waterfront station reported overhearing three teenagers bragging about having guns while on the platform. Metro police later stopped a train at the Anacostia station and located the three teenagers who matched the caller's description. Two of them were arrested on the scene, while a third fled and was arrested a short time later. The two 16−year−olds and one 17−year−old, all residents of the District, have been charged with carrying a pistol without a license and carrying ammunition.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=50057

[Return to top]

Postal and Shipping Sector

13. *June 09, DMNews* — **USPS board approves Bookspan NSA.** The U.S. Postal Service (USPS) Board of Governors has approved a negotiated service agreement (NSA) with Bookspan. The unanimous decision was filed June 1 with the Postal Rate Commission, and the NSA took effect that day. NSAs are special service and rate arrangements between the USPS and a mailer or group of mailers. Proponents say NSAs encourage greater volume by rewarding postal service customers with discounts and premium services. Bookspan joins Capital One, Bank One (now JPMorgan Chase), Discover Financial Services Inc. and HSBC North America Holdings Inc. in having approved NSAs. This NSA's volume−driven nature is particularly important to the USPS, said Mike Plunkett, manager of pricing strategy.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/37048.html

[Return to top]

Agriculture Sector

14. *June 09, Agricultural Research Service* — **Guarding corn and soybeans against viral attack.** A “viral strike force” in Wooster, OH, serves as the “front line” for spotting viral attacks on corn and soybeans in the U.S., and on corn worldwide. The team is jointly supported by the Agricultural Research Service (ARS) and The Ohio State University, Ohio Agricultural Research and Development Center in Wooster. Team members are being kept busy because Ohio has experienced an increase in soybean diseases in recent years. The latest emerging threat to soybeans in Ohio is bean pod mottle virus, which lowers yields and discolors the beans. Bean leaf beetles transmit the virus. ARS scientists are working to combine available partial virus resistance with beetle resistance to further slow the spread of the disease. They’ve developed a visual scoring system for rating symptoms of virus−infected plants on a scale of one to five and a diagnostic test to estimate the levels of virus in plants. These assays give them objective ways to measure the level of resistance to various viral diseases in corn and soybean plants and choose the most promising ones for breeding. The Wooster researchers will travel anywhere in the world, if invited to help identify a new corn virus.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

15. *June 06, United Press International* — **More than drought affecting wheat yields.** U.S. agronomists say wheat producers have more than a drought affecting their yields this year, as various viruses invade crops. Texas Agricultural Experiment Station researcher Tom Allen said he saw more than 150 wheat samples sent to the Great Plains Diagnostic Network lab this growing season, in addition to 400−plus samples the plant pathology staff gathered across the Panhandle. Ninety−five percent of the samples were diagnosed with the wheat streak mosaic virus. The virus is vectored by the wheat curl mite, Allen said, and so far there`s no treatment for either the virus or the mite. The samples came from as far north as Nebraska and as far south as Dallas, TX, making the outbreak the most widespread in years for wheat streak mosaic damage.
    Wheat streak mosaic virus information:
    http://www.uky.edu/Ag/Entomology/entfacts/fldcrops/ef117.htm
    Source: http://science.monstersandcritics.com/news/article_1170406.php/More_than_drought_affecting_wheat_yields

[Return to top]

Food Sector

16. *June 08, Associated Press* — **Dozens fall ill at restaurant in Arkansas.** More than two−dozen people became ill in Jonesboro, AR, after inhaling a substance believed to have been sprayed inside a restaurant, police said. Authorities were trying to determine the source of the substance that forced the restaurant's evacuation Tuesday, June 6. Some customers were gasping for air, and one complained of shortness of breath and a burning sensation in his nose and throat. Four were taken to hospitals, police said. "Due to the symptoms of the victims, it is believed that some substance, such as tear gas or some similar substance, may have been sprayed in the seating area of the restaurant," Patrolman Jonathan Landrum said.
    Source: http://www.breitbart.com/news/2006/06/08/D8I478G81.html

17. *June 08, Animal and Plant Health Inspection Service* — **Importation of untreated citrus from Mexico for processing in Texas allowed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Thursday, June 8, announced that it is allowing, under certain conditions, the importation of untreated citrus, such as grapefruit, sweet oranges and tangerines, from Mexico for processing in certain areas of Texas that are under quarantine for the Mexican fruit fly. To be eligible for importation, the fruit must originate from production sites in Mexico that participate in an APHIS−approved Mexican fruit fly preventive release program that uses sterile insects. APHIS−approved traps and lures must also be placed in production sites and a surrounding 1.5−mile buffer zone that will be monitored by APHIS. Each shipment must also be accompanied by phytosanitary certificate issued by Mexico's National Plant Protection Organization with additional declarations stating that the trapping requirements have been met. In addition, untreated Mexican citrus must be packed in insect−proof containers or covered with insect−proof mesh or plastic tarpaulin during its movement to Texas.
    Source: http://www.aphis.usda.gov/newsroom/content/2006/06/mxcitrus. shtml

18. *June 08, U.S. Food and Drug Administration* — **Self−heating containers recalled.** Lakeside Foods, Inc. is conducting a recall of all production codes of all products in 10 oz. self−heating

containers because the company recently learned that some cans may be contaminated with spoilage organisms or harmful bacteria due to seal leakage. There have been no reported illnesses associated with this product. Affected products reached consumers through a variety of distribution avenues including retail and grocery stores and the internet. This is a voluntary and precautionary action taken in cooperation with the U.S. Food and Drug Administration.
Source: http://www.fda.gov/oc/po/firmrecalls/lakeside06_06.html

[Return to top]

Water Sector

19. *June 08, Alamogordo Daily News (NM)* — **County put on emergency status.** Otero County, NM, has declared a state of emergency in Boles Acres, after the state health department ordered that the community's drinking water not be used at all. Paul Quarioli, county emergency services coordinator, said this morning that tests by the drinking water division of the state health department found evidence of both total coliform and E. coli bacteria in the Boles Acres water system. As a result, the system will be disinfected by state workers Friday, June 9. It will have to be allowed to set for several days, and then be tested again before residents can begin using the water, Quarioli said. The county is supplying temporary drinking water to residents at two locations in the community. The state of emergency and "no use" order was issued Monday, June 5, several days after heavy rains flooded sections of the community and contaminated the wells. State officials noted boiling the water probably wouldn't make it safe enough to drink.
Source: http://www.alamogordonews.com/apps/pbcs.dll/article?AID=/20060608/NEWS01/606080304/1001

[Return to top]

Public Health Sector

20. *June 10, New York Times* — **Polio takes unexpected toll in Namibia.** A fast−moving and deadly outbreak of polio has erupted in Namibia. The country had been free of polio for a decade. The outbreak is unrelated to the one that began spreading from Nigeria in 2004 through several countries in central Africa and the Arabian peninsula, and is unusual in that it is striking mostly adults, according to the World Health Organization. The disease has killed seven Namibians and paralyzed 33 more, driving panicked citizens to swarm hospitals seeking immunization. But because there was very little vaccine in sparsely populated Namibia −− only enough for routine vaccination of infants −− it quickly ran out, and people have been turned away. Once new shipments arrive the outbreak should be rapidly brought under control, said David Heymann, the WHO director general's representative for polio eradication. But Namibia's health minister said he did not expect to start a vaccination campaign until June 21. Polio normally attacks infants and young children, causing paralysis in only about one in 200 cases; in the rest, the virus causes no symptoms or only a mild, flu−like illness, and the infected child develops lifelong immunity. In adults, polio is more serious, and often paralyzes or kills.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.nytimes.com/2006/06/10/health/10polio.html?_r=1&h

p&ex=1149912000&en=510a6204c5e46fd4&ei=5094&partner=homepage &oref=slogin

21. *June 09, U.S. Food and Drug Administration* — **New measures to protect Americans from counterfeit drugs announced.** The U.S. Food and Drug Administration (FDA) Friday, June 9, announced new steps to strengthen existing protections against the growing problem of counterfeit drugs. The measures emphasize certain regulatory actions and the use of new technologies for safeguarding the integrity of the U.S. drug supply. Among other new measures, FDA will fully implement regulations related to the Prescription Drug Marketing Act of 1987, which requires drug distributors to provide documentation of the chain of custody of drug products. FDA had placed on hold certain regulatory provisions because of concerns raised at the time about the impact on small wholesalers. FDA also announces that, during the next year, its enforcement of drug tracking regulations will focus on products most susceptible to counterfeiting and diversion.
Source: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01386.html

22. *June 09, Reuters* — **Texas officials on lookout for tularemia.** An unusual number of dead jackrabbits in Texas has authorities concerned that tularemia could be making a comeback. The bacterial disease can infect humans but is rarely fatal. The latest case was confirmed recently in an area near Rick Husband International Airport in Amarillo, TX, according to Amarillo Bi−City−County Health District officials. Although no human cases have been reported from the most recent outbreak, there have been seven human cases of tularemia reported in Texas since 2002. People can contract the disease by direct contact with an infected animal or carcass via broken skin, the bite of an infected flea or tick, eating infected meat or inhaling the bacteria. "So far we have not found anything outside the original area where it was found," said Jim Alexander, regional Health Services zoonosis control veterinarian in Canyon, Texas. "We found some ticks and fleas off some of the original animals that were positive." Tularemia was a reportable disease in humans until 1992, when it was taken off the list. However, it was placed back on the list in 2002 due to bio−terrorism concerns, Alexander said.
Tularemia information: http://www.bt.cdc.gov/agent/tularemia/index.asp
Source: http://today.reuters.com/news/newsArticle.aspx?type=domestic News&storyID=2006−06−09T183128Z_01_N09167847_RTRUKOC_0_US−RA BBITS−TEXAS.xml&archived=False

23. *June 08, Reuters* — **Respiratory virus cases on rise in western U.S.** Between January and March of this year, health departments from Arizona, New Mexico, North Dakota, Texas, and Washington State reported an increased incidence of a respiratory viral infection, called human hantavirus pulmonary syndrome (HPS). D. Engelthaler, from the Arizona Department of Health Services, and associates confirm that nine cases of human HPS were documented between January and March, six of which occurred in Arizona and New Mexico. The years 1994 and 1999 were also characterized by a higher incidence of HPS during the first quarter, and subsequent increases in human HPS cases. During those years, increased rainfall during the previous year had caused increased vegetative biomass, which in turn promoted increased rodent populations susceptible to Hantavirus. So far, the only treatment for HPS is supportive care, and survival depends on early recognition, hospitalization, and intensive support. Even with treatment, human HPS has a mortality rate of 30 to 40 percent.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNe

ws&storyID=2006−06−09T005322Z_01_DIT903193_RTRUKOC_0_US−RESPIRATORY−VIRUS.xml

24. *June 08, Reuters* — **Officials test for bird flu in Alaska.** In a coastal marsh near the frozen Arctic Ocean, a black−and−white feathered spectacled eider leaves a gift for Corey Rossi, a wildlife biologist for the U.S. Department of Agriculture. Crouching down to take a closer look, Rossi inspects the dropping left by the large sea duck and then carefully dabs at the greenish mound with a swab before breaking off the tip into a plastic vial. The swab of eider dropping is one of 50,000 such field samples from wild birds that federal and local agencies aim to collect in the U.S. this year and test for the H5N1 strain of bird flu. Officials also want another 75,000 to 100,000 samples directly from the anus of live or dead birds. Barrow, AK, a crossroads for migratory birds from Asia −− is the front line for the government's efforts for early detection of bird flu's North American arrival.
Source: http://www.alertnet.org/thenews/newsdesk/N07343171.htm

25. *June 08, Democrat & Chronicle (NY)* — **State issues area health alert.** New York health officials are warning people who bought or came in contact with birds from a Wayne County pet store that they may have been exposed to psittacosis, a rare bacterial infection that can be transmitted to humans. State and county officials are investigating whether cockatiels purchased at the Animal Odyssey Pet Store in Newark may have infected three members of a Seneca County family. Psittacosis is a common disease among such pet birds as cockatiels, macaws, parrots and parakeets. In humans, the disease can cause fever, chills, muscle aches and even pneumonia, but is rarely fatal. If not properly treated, psittacosis can cause more severe illness in pregnant women. Transmission can occur while cleaning the bird droppings and inhaling the air. According to the state Health Department, one cockatiel purchased by the family died and another tested positive for psittacosis. Barbara Shipley, a superintendent of public health for the Wayne County Health Department, said the family reportedly visited the store over a period of several weeks before buying the bird that died. The store then replaced that bird with one that tested positive for the disease, she said.
Source: http://www.democratandchronicle.com/apps/pbcs.dll/article?AID=/20060608/NEWS01/606080342/1002/NEWS

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *June 09, U.S. Newswire* — **Joint commission study on emergency preparedness published.** A new study from the Joint Commission on Accreditation of Healthcare Organizations finds that community−based preparation for and response to disasters will require more effective communication and planning among hospitals, public health agencies and community first responders than currently exist. The study, “Integrating Hospitals into Community Emergency

Preparedness Planning," also found that national benchmarks are needed to measure and promote emergency preparedness planning. The study is the first large−scale national assessment of how closely hospitals and their communities are collaborating and planning together for natural or other disasters. Recent natural disasters and terrorist attacks have underscored the need for health care facilities to integrate their activities with community−based emergency preparedness efforts.
Study: http://www.annals.org/cgi/content/full/144/11/799
Source: http://releases.usnewswire.com/GetRelease.asp?id=67279

[Return to top]

Information Technology and Telecommunications Sector

27. *June 09, eWeek* — **No patch for critical Microsoft Windows 98 flaw.** One month before the expiration of support for Windows 98, Microsoft says it's simply "not feasible" to create patches for a critical flaw affecting the eight−year−old operating system. The vulnerability, patched for other Windows operating systems in the MS06−015 bulletin, exists in the way Windows Explorer handles Component Object Model (COM) objects but, although it puts Windows 98 users at risk of code execution attacks, Microsoft warned that a fix would not be made available. Public and technical support for Windows 98, Windows 98 SE (Second Edition), and Windows ME (Millennium Edition) formally ends on July 12. Microsoft's recommendation is for Windows 98 customers to protect those systems by placing them behind a perimeter firewall that filters traffic on TCP Port 139. This will block attacks attempting to exploit the Windows Explorer flaw.
Source: http://www.eweek.com/article2/0,1895,1974813,00.asp

28. *June 09, IDG News Service* — **Court upholds VoIP wiretapping.** A U.S. Federal Communications Commission (FCC) ruling requiring voice over Internet Protocol (VoIP) providers to give law enforcement agencies wiretapping capabilities is legal, a court ruled today. The U.S. Court of Appeals for the District of Columbia upheld the FCC's August 2004 ruling saying interconnected VoIP providers must allow wiretapping by May 14, 2007. Several groups had appealed the ruling, saying it could introduce security vulnerabilities into VoIP services and drive up costs for customers. The FCC ruling requires VoIP providers that offer a substitute service for traditional telephone service to comply with a 1994 telephone wiretapping law called the Communications Assistance for Law Enforcement Act.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001091

29. *June 09, Reuters* — **Microsoft to issue 12 patches for security flaws.** Microsoft plans to issue a dozen security alerts on Tuesday, June 13 −− some carrying the highest risk rating of critical −− as part of a monthly security update to fix flaws in its software. Nine of the patches relate to its Windows operating system, two address problems in its Microsoft Office productivity software and the other is for the company's Exchange e−mail server software.
Patches will be available for download at: http://www.microsoft.com/security
Source: http://today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2006−06−09T200523Z_01_N09371910_RTRUKOC_0_US−MICROSOFT−SECURITY.xml

30. *June 07, eWeek* — **Single agent desktop security comes of age.** Microsoft's impending move into the business PC security market is accelerating the development and adoption of so−called single agent desktop defense applications, according to many industry watchers. While the launch of the software giant's OneCare PC management service during the last week in May 2006 has already pushed rival security software makers to create their own bundled offerings for the home market, experts say that Microsoft's move into the enterprise security sector is similarly accelerating the development of centralized enterprise PC defense applications. Microsoft has already distributed a beta version of Microsoft Client Protection, a new security product that aims to help protect business desktops, laptops and file servers from a range of threats including viruses, spyware and rootkits, among other things. While single agent desktop security products are nothing new, the impending emergence of Microsoft Client Protection and demands from customers for integrated, easier−to−manage PC applications is driving traditional security software vendors to promote the tools more aggressively. Enterprise customer buying patterns, along with the demand for integrated security applications, are finally driving adoption of the technology.
Source: http://www.eweek.com/article2/0,1895,1970575,00.asp

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 − Symantec products vulnerable to buffer overflow:
http://www.kb.cert.org/vuls/id/4049100

Symantec Advisory SYM06−010 − Symantec Client Security and Symantec AntiVirus Elevation of Privilege:
http://securityresponse.symantec.com/avcenter/security/Conte nt/2006.05.25.htmll

US−CERT will advise as more information becomes available.

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is aware of an increase in activity attempting to exploit a vulnerability in Microsoft Word. The exploit is disguised as an email attachment containing a Microsoft Word document. When the document is opened, malicious code is installed on the user's machine. More information about the reported vulnerability

can be found in the following:

TRA06−139A − Microsoft Word Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−139A.htmll

VU#446012 − Microsoft Word buffer overflow:
http://www.kb.cert.org/vuls/id/446012

Review the workarounds described in Microsoft Security Advisory 919637:
http://www.microsoft.com/technet/security/advisory/919637.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines: Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html
Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 1027 (icq), 137 (netbios−ns), 1434 (ms−sql−m), 445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 113 (auth), 80 (www), 1433 (ms−sql−s) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer